

FILED JAN 18 11 00 AM '18

UNITED STATES DISTRICT COURT

for the
District of Oregon

In the Matter of the Search of)
 (Briefly describe the property to be searched)
 or identify the person by name and address))
 The premises located at 15139 SE Pine Court,)
 Portland, Oregon 97233, more fully described in)
 Attachment A hereto)

Case No. '18 -MC-27

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the _____ District of _____ Oregon (identify the person or describe property to be searched and give its location):

The premises located at 15139 SE Pine Court, Portland, Oregon 97233, more fully described in Attachment A hereto.

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

See Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of 18 U.S.C. § 2252A, and the application is based on these facts:

See the attached affidavit of Special Agent Seung Sung, U.S. Department of Homeland Security, Homeland Security Investigations (HSI).

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Seung H. Sung, Special Agent, HSI

Printed name and title

Sworn to before me and signed in my presence.

Date: Jan. 16, 2018



Judge's signature

City and state: Portland, Oregon

Honorable Stacie F. Beckerman, U.S. Magistrate Judge

Printed name and title

STATE OF OREGON)
) ss. AFFIDAVIT OF SEUNG SUNG
County of Multnomah)

I, Seung Sung, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent (SA) for the U.S. Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations (HSI) in Portland, Oregon. HSI is responsible for enforcing the customs laws, immigration laws, and federal criminal statutes of the United States. I am a law enforcement officer of the United States, and I am authorized by law to conduct investigations and to make arrests for felony offenses.

2. I have been a special agent with HSI since July 2002. My duties include the enforcement of federal criminal statutes prohibiting the sexual exploitation of children, including Title 18, United States Code, Sections 2251 through 2259, the Sexual Exploitation of Children Act (SECA). I have worked with agents involved in numerous investigations involving the sexual exploitation of children or the distribution, receipt, and possession of child pornography. I have participated in searches of premises and assisted in gathering evidence pursuant to search warrants, including in child pornography investigations. I graduated from the Criminal Investigator Training Program and Immigration and Customs Enforcement Special Agent Training, both held at the Federal Law Enforcement Training Center.

3. This affidavit is submitted in support of an application for a search warrant authorizing a search of the premises located at 15139 SE Pine Court, Portland, Oregon 97233, more fully described in Attachment A, for contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 2252A, as set forth in Attachment B.

4. The facts set forth in this affidavit are based on the following: my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; interviews of witnesses; my review of records related to this investigation; communications with others who have knowledge of the events and circumstances described herein; and information gained through my training and experience. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of an application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

Statutory Authority

5. Title 18, United States Code, Section 2252A(a)(1) prohibits a person from knowingly transporting or shipping child pornography using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means, including by computer.

6. Title 18, United States Code, Sections 2252A(a)(2)(A) and (b)(1) prohibit a person from knowingly receiving or distributing any material containing child pornography that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or conspiring or attempting to do so.

7. 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or accessing with intent to view any child pornography that has been mailed, shipped, or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using

materials that were mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or attempting to do so.

Definitions

8. The following definitions apply to this affidavit and to Attachment B:

a) “Child erotica” means materials or items that are sexually arousing to persons having a sexual interest in children but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.

b) “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

c) “Internet Service Providers” (“ISPs”) are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

d) “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

e) “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

f) “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) the lascivious exhibition of the genitals or pubic area of any person.

g) “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

Background on Computers and Child Pornography

9. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the knowledge, experience, and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have dramatically changed the manner in which child pornography is produced and distributed.

10. Digital cameras and video recorders (including those found on many smart phones) readily and easily allow for the production of child pornography. Using digital cameras or video recorders, images and videos of child pornography can be uploaded directly onto a computer, where they can easily be edited, manipulated, copied, and distributed. A paper photograph can be digitized and uploaded to a computer through the use of a scanner. Once uploaded, such photographs can be edited, manipulated, copied, and distributed just like any other digital image. A modem allows any computer to connect to another computer through the

use of a telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to millions of computers around the world.

11. The computer's ability to store images in digital form makes it an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, a wide variety of removable digital data storage media exist which add additional storage capacity, and which provide a portable platform on which to store and transport child pornography. Examples of such removable storage media include external hard drives, thumb drives, flash drives, and secure digital data cards, some of which are quite small, are highly portable, are easily concealed, and are often carried on a subject's person. Smart phones are also often used to access the Internet, and to produce, transport, receive, store, and view child pornography. An individual using a smart phone can easily plug the device into a computer, via a USB cable, and transfer data files from one digital device to another. Smart phones are relatively small, are highly portable, and are often carried on a subject's person.

12. The Internet affords individuals who collect and trade in child pornography several different venues for meeting each other, and for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Such venues include chat rooms, bulletin board services, social networking sites, instant messaging services, and peer-to-peer (P2P) file sharing networks.

13. Individuals also use online resources to store and retrieve child pornography, including services offered by Internet portals such as Yahoo!, Hotmail, Google, and others. Such

online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer.

14. Typically, computers or devices on the Internet are referenced by a unique Internet Protocol (IP) address, much like a telephone has a unique telephone number. Each time an individual accesses the Internet, the computer or device from which that individual initiates access is assigned an IP address by the individual's Internet Service Provider. An IP address may be statically assigned, meaning the individual is assigned the same IP address each time he or she accesses the Internet. An IP address may also be dynamically assigned, meaning that a user may receive a different IP address each time he or she accesses the Internet. Internet service providers typically log the date, time, and duration of the Internet session for each IP address and can identify the subscriber of that IP address for such a session from those records.

15. Digital information, including communications to and from a computer, is often saved or stored on a computer. Storing this information can be intentional, for example by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. For example, a forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the

files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools.

16. When a person deletes a file on a computer, the data contained in the file ordinarily does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits.

17. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals involved in collecting and trading child pornography:

a. Individuals who collect and trade in child pornography frequently store their collections on computers and digital storage media, which they keep in secure locations, such as their residences. Such persons typically keep their collections of child pornography close at hand, and often retain their collections for extended periods of time. Such persons treat their collections as prized possessions, rarely disposing of them entirely. In some recent cases, however, such persons have been found to download and delete child pornography on a cyclical and repetitive basis, rather than storing a collection indefinitely.

b. Such persons also may correspond with and/or meet others to share information and materials; conceal such correspondence as they do their sexually explicit material; and often maintain contact information for individuals who share an interest in child pornography.

c. Such persons prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

d. In the case of those who collect and trade child pornography via email, the nature of email itself provides a convenient means by which these individuals can access their collections from any computer, at any location with Internet access. These individuals therefore do not need to physically carry their collections with them, but rather can access them electronically. Furthermore, these collections can be stored on email “cloud” servers that allow users to store a large amount of material at little or no cost, thus eliminating the need to store child pornography collections on the users’ own computers.

Background on the BitTorrent Peer-to-Peer File Sharing Network

18. Based on my training and experience, I know the following regarding P2P file sharing networks, including the BitTorrent network.

a. P2P file sharing programs allow groups of computers using the same file sharing network and protocols to transfer digital files from one computer to another while connected to a network. Different P2P file sharing networks on the Internet use different file sharing protocols.

b. To connect to a particular P2P file sharing network, a user first downloads a P2P client software program. Once the software is installed, the user designates the files to be shared by placing them in a “shared files” folder. The user can search for and download particular files from other users, just as other users can search for and download files the user is making available for sharing. Some P2P client software programs allow portions of a file to be shared with others during the download process. Some P2P client software programs allow the user to opt out of sharing, or to limit how others can obtain files from the user.

c. P2P client software processes each file being offered by a user and creates a “hash value” for each. A hash value is a mathematical algorithm that uniquely identifies a file based on its content, and is akin to a “digital fingerprint” or the “digital DNA” of a file. Two files with matching hash values are considered identical, even if the files have different file names. P2P client software uses hash values to download parts of files from multiple computers on the network (a process known as “multiple source downloading”), then reassembles the file on the user’s computer. Multiple source downloading speeds up downloading times

considerably, and makes the P2P network run more efficiently. Multiple source downloading only works if the files from which the various parts are taken have matching hash values.

d. The BitTorrent network is a very popular, publically available P2P file sharing network. The BitTorrent network can be accessed by computers running many different client programs, including the BitTorrent client program, the uTorrent client program, and the Vuze client program. Those programs are free and are publically available on the Internet.

e. During installation, the user designates one or more directories or folders whose files will be available to other BitTorrent network users to download. In order to share a file or a set of files on the BitTorrent network, a user creates a “torrent” file. A torrent is typically a small file that describes the files being shared, including file names, an “info hash” value, and how to locate the files on the BitTorrent network, but does not contain the actual files. The “info hash” is a hash value of the set of data describing the files referenced in the torrent, which include the hash value of each file piece, the file size, and the file names. The “info hash” of each torrent uniquely identifies the torrent file on the BitTorrent network.

f. A torrent file may also contain information on how to locate files referenced in the torrent by identifying “trackers.” “Trackers” are computers on the BitTorrent network that collate information about peers that have recently reported they are sharing the files referenced in the torrent file. A tracker is a pointer to peers on the network who may be sharing part or all of the file(s) referenced in the torrent. Trackers do not actually contain the files being shared. There are many publically available servers on the Internet that provide BitTorrent tracker services.

g. To locate torrent files of interest, a user can enter keyword searches within the BitTorrent network client itself or on websites hosting torrents. Once a user finds a torrent file that meets the keyword search criteria, the user downloads the torrent file. The BitTorrent network client then processes the torrent file in order to find peers on the network that have all or part of the files referenced in the torrent file. The actual files referenced in the “Torrent” are obtained directly from other peers on the BitTorrent network.

h. P2P networks, including the BitTorrent network, are frequently used to trade digital files containing child pornography. A user interested in obtaining child pornography on the BitTorrent network can conduct a keyword search using terms typically associated with child pornography. The search results are typically returned to the user’s computer by displaying them on a torrent hosting website. The hosting website typically displays information about the torrent, including the name of the torrent file, the names of files referenced in the torrent file, the file sizes, and the “info hash” value of the torrent file. The user selects a torrent of interest and downloads it to their computer. The BitTorrent client program then processes the torrent file. The user selects the files in the torrent the user wants to download. The BitTorrent client program will then locate peers who have the desired files (or parts of the files), and will download the files directly from those peer computers. Typically, once the BitTorrent network client has downloaded part of a file, it is immediately available for sharing with other users on the network. During the download process, a typical BitTorrent client program displays the Internet Protocol address(es) of the peer(s) who are sharing part or all of the files being downloaded. The downloaded files, including the torrent file, will remain in the designated download folder on user’s computer until they are moved or deleted.

i. Law enforcement has created BitTorrent network client programs that obtain information from trackers about users who recently reported sharing digital files known (based on the files' hash values) to contain child pornography. The law enforcement client programs are designed to download files from a single IP address (as opposed to obtaining the file from multiple peers/clients on the network).

j. During the query and downloading process, certain information may be exchanged between the law enforcement client program and the remote client the investigator is querying or downloading a file from. Such information includes: (1) the remote client's IP address; (2) a confirmation from the remote client that they have and are sharing pieces of the files being requested; and 3) the remote client program and version. The investigator can log that information. In addition, that information may remain on the remote client's computer system for a long time. A forensic examination of a seized computer can reveal that information, which can be further evidence that the investigator's client communicated with the remote client.

Statement of Probable Cause

19. On June 22, 2017, HSI SA Julie Peay was conducting an online investigation on the BitTorrent network for offenders sharing child pornography. SA Peay used undercover investigative software to identify a user at IP address 184.100.204.163, who was associated with a torrent with the infohash: 4f8553f3a984b40e53c0cfdb0606e9084f447709. This torrent file references 88 files, at least one of which was identified as being a file of investigative interest to child pornography investigations. A file of investigative interest is one whose hash value has been linked to a child pornography investigation. Many but not all such files are child pornography.

20. Using a computer running a law enforcement version of the BitTorrent client software, SA Peay directly connected to a device at IP address 184.100.204.163, hereinafter referred to as the “suspect device.” The suspect device reported it was using BitTorrent client software UT2210 µTorrent 2.2.1.

21. On June 22, 2017, between 3:30 am 6:00 am, SA Peay successfully downloaded 43 files from the suspect device at IP address 184.100.204.163. The suspect device was the only candidate for each download. SA Peay downloaded each file directly from that IP address.

22. On September 27, 2017, I received copies of each of the files SA Peay downloaded. I reviewed those files, and determined that the majority of them depicted child pornography. Description of four of the files follows.

a. Adry Blowjob1-1.MTS_thumbs_(2014.05.19_21.02.24).jpg (hash value NLS67LR2IZS6U5GP4KH53ZVRQVFDCOEO): This file contains 16 images of a prepubescent girl performing oral sex on an adult male’s erect penis. The adult male is lying down, and is wearing blue shorts/pants.

b. Adry Play With dely and Dad
(5).MTS_thumbs_(2014.05.19_21.58.15).jpg (hash value PBAYIA4MCLFEO35ULFPV4Z7Q6DEOLEXY): This file contains 2 images. The first image depicts a naked prepubescent girl sitting on a bed while a second prepubescent girl is on her knees next to the bed, performing oral sex on an adult male. The second image is a partial image of a naked prepubescent girl sitting on a bed while a second prepubescent girl is on her knees, holding an erect adult penis in her right hand.

c. Tropical-Adry-hc2.jpg (hash value E2ZR6AG4MRB73LUB3JJDWBMF37XKKERH): This file contains 16 images depicting a naked prepubescent girl either holding or performing oral sex on an erect adult penis.

d. Tropical-Adry-hc9.jpg (hash value U5M2VSWUZ3DGYDDZMSUUOVWAODX4EGRD): This file contains 16 images of a naked prepubescent girl and a naked adult male. Some of the images depict the girl sitting on top of the naked adult male, having sexual intercourse with him. Other images show the adult male performing oral sex on the prepubescent girl.

23. The IP address 184.100.204.163 belongs to the ISP CenturyLink. On or about July 20, 2017, Homeland Security Investigations (HSI) issued an administrative summons to CenturyLink for subscriber information and the port number for that IP address at the time of SA Peay's downloads. On July 26, 2017, in response to the subpoena, CenturyLink provided the following subscriber information:

Subscriber Name: Sherrie Amaral
Service Address: 15139 SE Pine Ct.
Portland CO [sic]
Billing address: Sherrie Amaral
PO BOX 33804
Portland, OR 97292
User ID: amaralsherrie
Type of Service: High Speed Internet Service
Account Number: 5032569931126
Start of Service: 01/13/2016
Account Status: Active
IP Assignment: Dynamic DSL IP

24. On or about August 17, 2017, Century Link had previously stated that subscriber information is associated by IP address only, so they could not provide a port number.

25. Queries conducted in commercial databases revealed that Sherrie Auliilokelani Amaral (DOB XX-XX-77) and Brian James Tucker (DOB XX-XX-83) are associated with 15139 SE Pine Court, Portland, Oregon 97233. In addition, Amaral's and Tucker's Oregon driver's licenses both list addresses of 15139 SE Pine Court, PTL D, and PO Box 33804, Portland, OR 97292.

26. On or about October 6, 2017, a check of Oregon Department of Motor Vehicles records revealed that Sherrie Auliilokelani Amaral and Brian James Tucker have vehicles registered in their names at 15139 SE Pine Ct., PTL D, and PO Box 33804, Portland, OR, 97292.

27. According to a law enforcement database, neither Sherrie Auliilokelani Amaral nor Brian James Tucker has any known criminal history.

28. On or about October 13, 2017, I drove to 15139 SE Pine Ct., Portland, Oregon 97233, and took photographs of the exterior of the residence. The residence is a two story single family residence with brownish color siding and white trim. The residence has a composite roof and a one car garage. The front door is red and faces north. The black numbers "15139" are affixed to the right side of the garage door.

29. On that same date, I observed a silver Acura bearing Oregon license 390HAA leave the residence. That vehicle is registered to Brian Tucker at 15139 SE Pine Ct., PTL D.

30. On that same date, I parked on the street in front of 15139 SE Pine Ct. and scanned for wireless networks using a mobile device. I did not see any unsecured wireless networks.

31. On or about October 16, 2017, the U.S. Postmaster informed me that Sherrie Amaral is the primary subscriber of PO Box 33804, Portland Oregon 97292, and Brian Tucker is listed as an authorized user of the PO Box. Amaral list a physical address of 15139 SE Pine Court, Portland Oregon 97233. The PO Box was opened on 04/26/17.

32. On or about October 20, 2017, in response to an administrative summons, Portland General Electric (PGE) advised the electric service at 15139 SE Pine Court, Portland, Oregon 97233 is listed in their records under the address 308 SE 151st Ave., Portland Oregon 97233. The subscriber information for that account is as follows:

Customer name:	Amaral, Sherrie
SSN:	XXX-XX-2239
DOB:	XX/XX/1977
Driver's License:	XXX1769
Employer:	State of Oregon
Telephone:	xxx-xxx-7797
Service dates:	04/24/2013- present

33. PGE stated that the previous owner of that property called them on June 18, 2009, to advise that the address of that residence should be updated to 15139 SE Pine Court, Portland Oregon 97233, and that 308 SE 151st Ave., Portland Oregon 97233, was no longer a valid address. PGE never updated the address in their records. Accordingly, the customer's account is still listed under 308 SE 151st Ave., Portland Oregon 97233.

34. According to Multnomah County property tax records, the property at 308 SE 151st Avenue was divided into five separate parcels. One of those parcels is 15139 SE Pine Court. Multnomah County tax records list the owner of 15139 SE Pine Court as Sherrie Amaral, with a purchase date of April 24, 2013.

Search and Seizure of Digital Data

35. This application seeks permission to search for and seize evidence of the crimes described above, including evidence of how computers, digital devices, and digital storage media were used, the purpose of their use and who used them.

36. Based upon my training and experience, and information related to me by agents and others involved in the forensic examination of computers and digital devices, I know that data in digital form can be stored on a variety of systems and storage devices, including hard disk drives, floppy disks, compact disks, magnetic tapes, flash drives, and memory chips. Some of these devices can be smaller than a thumbnail and can take several forms, including thumb drives, secure digital media used in phones and cameras, personal music devices, and similar items.

Removal of Data Storage Devices

37. I know that a forensic image is an exact physical copy of a data storage device. A forensic image captures all data on the subject media without viewing or changing the data in any way. Absent unusual circumstances, it is essential that a forensic image be obtained prior to conducting any search of data for information subject to seizure pursuant to the warrant. I also know that during a search of premises it is not always possible to create a forensic image of or search digital devices or media for data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. Because there are so many different types of digital devices and software in use today, it is difficult to anticipate all of the necessary technical

manuals, specialized equipment, and specific expertise necessary to conduct a thorough search of the media to ensure that the data will be preserved and evaluated in a useful manner.

b. Searching digital devices can require the use of precise, scientific procedures designed to maintain the integrity of the evidence and to recover latent data not readily apparent to the casual user. The recovery of such data may require the use of special software and procedures, such as those used in a law enforcement laboratory.

c. The volume of data stored on many digital devices is typically so large that it is generally highly impractical to search for data during the execution of a physical search of premises. Storage devices capable of storing 500 gigabytes to several terabytes of data are now commonplace in desktop computers. It can take several hours, or even days, to image a single hard drive. The larger the drive, the longer it takes. Depending upon the number and size of the devices, the length of time that agents must remain onsite to image and examine digital devices can become impractical.

Laboratory Setting May Be Essential For Complete and Accurate Analysis Of Data

38. Since digital data may be vulnerable to inadvertent modification or destruction, a controlled environment, such as a law enforcement laboratory, may be essential to conduct a complete and accurate analysis of the digital devices from which the data will be extracted. Software used in a laboratory setting can often reveal the true nature of data. Therefore, a computer forensic reviewer needs a substantial amount of time to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband, or an instrumentality of a crime.

39. Analyzing the contents of a computer or other electronic storage device, even without significant technical difficulties, can be very challenging, and a variety of search and analytical methods must be used. For example, searching by keywords, which is a limited text-based search, often yields thousands of hits, each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant hit does not end the review process. The computer may have stored information about the data at issue which may not be searchable text, such as: who created it; when and how it was created, downloaded, or copied; when it was last accessed; when it was last modified; when it was last printed; and when it was deleted. The relevance of this kind of data is often contextual. Furthermore, many common email, database, and spreadsheet applications do not store data as searchable text, thereby necessitating additional search procedures. To determine who created, modified, copied, downloaded, transferred, communicated about, deleted, or printed data requires a search of events that occurred on the computer in the time periods surrounding activity regarding the relevant data. Information about which users logged in, whether users shared passwords, whether a computer was connected to other computers or networks, and whether the users accessed or used other programs or services in the relevant time period, can help determine who was sitting at the keyboard.

40. *Latent Data:* Searching digital devices can require the use of precise, scientific procedures designed to maintain the integrity of the evidence and to recover latent data. The recovery of such data may require the use of special software and procedures. Data that represents electronic files or remnants of such files can be recovered months or even years after it has been downloaded onto a hard drive, deleted, or viewed via the Internet. Even when such

files have been deleted, they can be recovered months or years later using readily available forensic tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in space on the hard drive or other storage media that is not allocated to an active file. In addition, a computer's operating system may keep a record of deleted data in a swap or recovery file or in a program specifically designed to restore the computer's settings in the event of a system failure.

41. *Contextual Data:*

a. In some instances, the computer "writes" to storage media without the specific knowledge or permission of the user. Generally, data or files that have been received via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to such data or files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve artifacts of electronic activity from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer usage. Logs of access to websites, file management/transfer programs, firewall permissions, and other data assist the examiner and investigators in creating a "picture" of what the computer was doing and how it was being used during the relevant time in question. Given the interrelationships of the data to various parts of the computer's operation, this information cannot be easily segregated.

b. Digital data on the hard drive that is not currently associated with any file may reveal evidence of a file that was once on the hard drive but has since been deleted or

edited, or it could reveal a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, email programs, and chat programs store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, can indicate the identity of the user of the digital device, or can point toward the existence of evidence in other locations. Such data may also lead to exculpatory evidence.

c. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be learned from the absence of particular data on a digital device. Specifically, the lack of computer security software, virus protection, malicious software, evidence of remote control by another computer system, or other programs or software, may assist in identifying the user indirectly and may provide evidence excluding other causes for the presence or absence of the items sought by this application. Additionally, since computer drives may store artifacts from the installation of software that is no longer active, evidence of the historical presence of the kind of software and data described may have special significance in establishing timelines of usage, confirming the identification of certain users, establishing a point of reference for usage and, in some cases, assisting in the identification of certain users. This data can be evidence of a crime, can indicate the identity of the user of the digital device, or can point toward the existence of evidence in other locations. Such data may also lead to

exculpatory evidence. Evidence of the absence of particular data on the drive is not generally capable of being segregated from the rest of the data on the drive.

Search Procedure

42. In searching for data capable of being read, stored, or interpreted by a computer or storage device, law enforcement personnel executing the search warrant will employ the following procedure:

a. *On site search, if practicable.* Law enforcement officers trained in computer forensics (hereafter, “computer personnel”), if present, may be able to determine if digital devices can be searched on site in a reasonable amount of time and without jeopardizing the ability to preserve data on the devices. Any device searched on site will be seized only if it contains data falling within the list of items to be seized as set forth in the warrant and in Attachment B.

b. *On site imaging, if practicable.* If a digital device cannot be searched on site as described above, the computer personnel, if present, will determine whether the device can be imaged on site in a reasonable amount of time without jeopardizing the ability to preserve the data.

c. *Seizure of digital devices for off-site imaging and search.* If no computer personnel are present at the execution of the search warrant, or if they determine that a digital device cannot be searched or imaged on site in a reasonable amount of time and without jeopardizing the ability to preserve data, the digital device will be seized and transported to an appropriate law enforcement laboratory for review.

d. Law enforcement personnel will examine the digital device to extract and seize any data that falls within the list of items to be seized as set forth in the warrant and in Attachment B. To the extent they discover data that falls outside the scope of the warrant that they believe should be seized (e.g., contraband or evidence of other crimes), they will seek an additional warrant.

e. Law enforcement personnel will use procedures designed to identify items to be seized under the warrant. These procedures may include the use of a “hash value” library to exclude normal operating system files that do not need to be searched. In addition, law enforcement personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized under the warrant.

f. If the digital device was seized or imaged, law enforcement personnel will perform an initial search of the original digital device or image within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If, after conducting the initial search, law enforcement personnel determine that an original digital device contains any data falling within the list of items to be seized pursuant to the warrant, the government will retain the original digital device to, among other things, litigate the admissibility/authenticity of the seized items at trial, ensure the integrity of the copies, ensure the adequacy of chain of custody, and resolve any issues regarding contamination of the evidence. If the government needs additional time to determine whether an original digital device or image contains any data falling within the list of items to be seized pursuant to this warrant, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete the search of the digital device or image within 180

days of the date of execution of the warrant. If the government needs additional time to complete the search, it may seek an extension of the time period from the Court within the original 180-day period from the date of execution of the warrant.

g. If, at the conclusion of the search, law enforcement personnel determine that particular files or file folders on an original digital device or image do not contain any data that fall within the list of items to be seized pursuant to the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the list of items to be seized pursuant to the warrant, as well as data within the operating system, file system, or software application relating or pertaining to files or data falling within the list of items to be seized pursuant to the warrant (such as log files, registry data, and the like), through the conclusion of the case.

h. If an original digital device does not contain any data falling within the list of items to be seized pursuant to this warrant, the government will return that original data device to its owner within a reasonable period of time following the search of that original data device and will seal any image of the device, absent further authorization from the Court.

Items to be Seized

43. In order to search for data that is capable of being read or interpreted by a computer, law enforcement personnel will need to seize, image, copy, and/or search the following items, subject to the procedures set forth herein:

a. Any computer equipment or digital devices that are capable of being used to commit or further the crimes outlined above, or to create, access, or store the types of contraband and evidence, fruits, or instrumentalities of such crimes, as set forth in Attachment B;

b. Any computer equipment or digital devices used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners that are capable of being used to commit or further the crimes outlined above, or to create, access, process, or store the types of contraband and evidence, fruits, or instrumentalities of such crimes, as set forth in Attachment B;

c. Any magnetic, electronic, or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD ROMs, CD-Rs, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, personal digital assistants, iPods, and cell phones capable of being used to commit or further the crimes outlined above, or to create, access, or store the types of contraband and evidence, fruits, or instrumentalities of such crimes, as set forth in Attachment B;

d. Any documentation, operating logs, and reference manuals regarding the operation of the computer equipment, storage devices, or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. Any physical keys, encryption devices, dongles, or similar physical items which are necessary to gain access to the computer equipment, storage devices, or data;

g. Any passwords, password files, test keys, encryption codes, or other information necessary to access the computer equipment, storage devices, or data; and

h. All records, documents, programs, applications, or materials created, modified, or stored in any form, including in digital form, on any computer or digital device, that show the actual user(s) of the computers or digital devices during any time period in which the device was used to upload, download, store, receive, possess, or view child pornography, including the web browser's history; temporary Internet files; cookies, bookmarked or favorite web pages; email addresses used from the computer; MAC IDs and/or Internet Protocol addresses used by the computer; email, instant messages, and other electronic communications; address books; contact lists; records of social networking and online service usage; and software that would allow others to control the digital device such as viruses, Trojan horses, and other forms of malicious software.

Retention of Image

44. The government will retain a forensic image of each electronic storage device subjected to analysis for a number of reasons, including proving the authenticity of evidence to be used at trial; responding to questions regarding the corruption of data; establishing the chain of custody of data; refuting claims of fabricating, tampering with, or destroying data; and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

Inventory and Return

45. With respect to the seizure of electronic storage media or the seizure or imaging of electronically stored information, the search warrant return to the Court will describe the physical storage media that were seized or imaged.

46. The government has made no prior effort in any judicial forum to obtain the materials sought in this requested warrant.

Conclusion

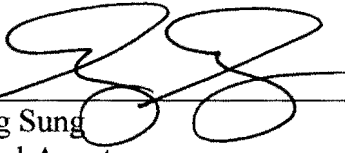
47. Based on the foregoing, I have probable cause to believe someone at the premises located at 15139 SE Pine Ct., Portland Oregon 97233, committed the offenses of transportation, distribution, and possession of child pornography, and that contraband and evidence, fruits, and instrumentalities of those violations, as more fully described in Attachment B, may be located therein. I therefore respectfully request that the Court issue a warrant authorizing a search of those premises, more fully described in Attachment A, for the items listed in Attachment B, and authorizing the seizure and examination of any such items found.

///

///

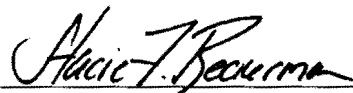
///

48. This affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorney (AUSA) Gary Sussman prior to being submitted to the Court. AUSA Sussman informed me that in his opinion, the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.



Seung Sung
Special Agent
Homeland Security Investigations

Sworn and subscribed before me this 16th day of January 2018.



Honorable Stacie F. Beckerman
United States Magistrate Judge